



GEORGETOWN LAW

Paul Ohm
Professor of Law

July 28, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th St., SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other
Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch,

On July 26, 2016, in regard to the above captioned proceeding, I met with Gigi Sohn, Counselor to the Chairman; Scott Jordan, Chief Technologist; Lisa Hone, Associate Bureau Chief of the Wireline Competition Bureau; Daniel Kahn, Chief of the Competition Policy Division within the Wireline Competition Bureau; Melissa Kinkel, Assistant Chief of the Competition Policy Division within the Wireline Competition Bureau; Jonathan Mayer, Chief Technologist of the Enforcement Bureau; Eric Feigenbaum, Director of Outreach & Strategy from the Office of Media Relations; and from the Competition Policy Division within the Wireline Competition Bureau, the following additional attorneys: David Brody, Alex Espinoza, Heather Hendrickson, Brian Hurley, Bakari Middleton, and Sherwin Siy.

At this meeting, I discussed the need for a strong requirement for deidentification in the Commission's broadband privacy rule, both as a matter of statutory interpretation and sound policy; and the difficulty and inappropriateness of drawing lines distinguishing between sensitive and non-sensitive information.

Statutory Interpretation

Section 222¹ should properly be read to establish a binary dichotomy between "individually identifiable customer proprietary network information" and "aggregate

¹ 47 U.S.C. § 222.

customer information.” Any information born as CPNI, even when deidentified, falls only within one of those two categories. This is by far a more natural reading of the statute than the contrary interpretation, advanced by some industry commenters, identifying a third category of “not individually identifiable” but also “not aggregate” information, which presumably would fall outside the strictures of the statute.

A plain reading of the statute supports the “two categories” interpretation. Congress chose an obvious and self-evident parallel construction in the key subsections. Subsection 222(c)(1) provides:

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to *individually identifiable customer proprietary network information* in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

While subsection 222(c)(3) provides:

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to *aggregate customer information* other than for the purposes described in paragraph (1).

The parallel construction is striking. I have adorned the text above with parallel text styles to indicate identical or nearly-identical phrases (underlined) and to highlight passages that are not identical but sit at parallel positions (bolded or bold-italicized). This formatting isolates the key parallel phrases (bold-italicized): “individually identifiable [CPNI]” and “aggregate customer information.” The lockstep placement of these two phrases in precisely the same location in the respective subsections, serving precisely the same role, suggests strongly that Congress regarded these two phrases as alternative choices to one another. Information can be either “aggregate” or “individually identifiable.” There is no room in the statute for a third category.

This interpretation is supported further in the definition of “aggregate customer information,” which means “collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.”² The focus on “individual customer identities and characteristics” suggests that Congress considered this category to be the opposite of individually identifiable CPNI.

This also explains why Congress chose not to define “individually identifiable CPNI,” as the phrase should be implicitly understood as anything falling outside the defined term, aggregate customer information. It would have been redundant and thus unnecessary to have defined a term that means only the opposite of another term.

Far from rendering “individually identifiable” mere surplusage, as some have contended a “two categories” reading would do, this interpretation explains the use of this modifier. Congress envisioned an overarching category of CPNI, which would occur as either individually identifiable CPNI or aggregate customer information without the possibility for a third option.

² 47 U.S.C. § 222(h)(2).

The Need for a Strong Deidentification Standard

Even if there were room in the statute to construct a third category of non-individually identifiable information that is not aggregate, the Commission would be advised to find that this category encompasses only the most rigorously deidentified information. Subsection 222(c)(1) refers to “individually identifiable” CPNI—not “*reasonably* individually identifiable” CPNI. The unadorned phrase “individually identifiable” means, quite literally, information that can possibly be identified with an individual. The most natural reading of non-individually identifiable information would therefore be “not possible to reidentify” and would not cover any information that could be reidentified as an absolute, technical matter, regardless of business process protections that might reduce the risk of reidentification.

This statutory interpretation would also represent the best result from a policy standpoint. As I have elaborated at length in my two recent statements to Congress about these proceedings, Section 222 represents the legislative conclusion that telecommunications providers should be subject to strict privacy requirements.³ Specifically, the Commission should continue to adhere to its proposed standard in the NPRM defining deidentification as information that is “not reasonably linkable to a specific individual”⁴ or not “linked or linkable to an individual”.⁵

One virtue of adopting a standard of “not linked or linkable to an individual” is it follows the lead of the FTC. Contrary to what some commenters would like the Commission to believe, rigorous deidentification requirements are consistent with the standard specified in the FTC’s 2012 Privacy Report.⁶ The FTC report speaks only of technical rather than process protections.⁷ I have always regarded the FTC’s definition to be a very aggressive and appropriately strong form of deidentification, one that speaks of the need for technological rather than business process protections. Many commenters, most notably the Future of Privacy Forum (an industry trade association), have engaged in a multi-year, well-funded crusade to reinterpret the FTC’s test as weak and watered-down. The Commission should understand this effort for what it is: an exercise in creative reinterpretation.

³ Statement of Paul Ohm before the United States Senate Committee on Commerce, Science, and Transportation (July 12, 2016), *available at* <http://paulohm.com/projects/testimony/PaulOhm20160712FCCPrivacyRulesSenate.pdf>; Statement of Paul Ohm before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives (June 14, 2016), *available at* <http://paulohm.com/projects/testimony/PaulOhm20160614FCCPrivacyRules.pdf>.

⁴ *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500, 2607 § 64.7002(g)(1) (2016).

⁵ *Id.* at 2602 § 64.2003(o).

⁶ FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 18-22 (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁷ *Id.* at 21 (“Depending on the circumstances, a variety of *technical approaches* to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient “noise” to data, statistical sampling, or the use of aggregate or synthetic data.”) (emphasis added).

Drawing Lines Based on Sensitivity

The Commission should resist calls to require opt-in consent only for sensitive information, for at least four reasons: First, the design of the statute makes clear that all covered information is intrinsically sensitive. Second, given the difficulty in defining what is meant by sensitive, any rule that turned on this distinction would be a rule that was so poorly defined as to give the consumer no assurances about when their activity was protected or not. Third, because the statute provides a broad exception for customer consent, the onus should be on industry actors who want to use nonsensitive information for secondary purposes, not on customers who would prefer they did not. Finally, the idea that we can define sensitivity by multistakeholder committee stands as perhaps the most wrong-headed proposal in this entire proceeding.

First, when Congress enacts a sectoral privacy law, which Section 222 is, it reflects Congressional judgment that information covered by the sector is intrinsically sensitive. It tends not in these situations to draw fine lines based on levels of sensitivity. So, for example, HIPAA protects all health information, regardless of sensitivity. Private communications are subject to protection under the Wiretap Act, not only when those conversations are deemed sensitive. And student records are protected by FERPA, regardless of sensitivity.

Second, as I have investigated in a recent article, it is very difficult to define whether information is sensitive.⁸ The sensitivity of information depends on context. What is sensitive to one person may be not-so-sensitive to another. As a case in point, six years ago, I authored an article about the surprising power of reidentification.⁹ I chose as a principal example, reidentification attacks on databases of movie ratings released by Netflix. At the time, some respondents challenged the importance of this example by asking me, “who cares who knows the list of movies I have watched?” Shortly after my article, lawyers filed a class-action lawsuit against Netflix, identifying as its class representative an in-the-closet lesbian Jane Doe plaintiff who felt that her sexual orientation could be revealed to neighbors who had access to her Netflix viewing record. She asserted in the lawsuit complaint that “were her sexual orientation public knowledge, it would negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children’s ability to live peaceful lives.”¹⁰

The deeply contextual and personal nature of individual sensitivity means that an ISP would be obligated to develop a contextual picture of each customer in order to make accurate decisions about sensitivity. An ISP would either need to erect a comprehensive surveillance apparatus in order to develop a richer understanding of each customer, in order to make more nuanced prediction of each person’s sensitivities, obliterating privacy along the way; or it would ignore the surrounding context, defining sensitivity crudely and non-scientifically, subjecting customers to wildly under- and over-protective line drawing.

Third, there is no real need to draw lines based on sensitivity of data because the statute at issue here—and the rule proposed by the Commission—establishes broad exceptions for customer consent. As I explained in my reply comment in this proceeding, the

⁸ Paul Ohm, *Sensitive Information*, 80 S. CAL. L. REV. 1125 (2015).

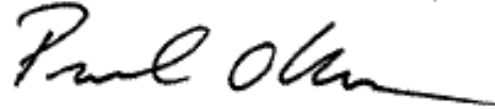
⁹ Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

¹⁰ Doe v. Netflix, Class Action Complaint, Case No. C09-05903, at 21 (Dec. 17, 2009), available at http://www.wired.com/images_blogs/threatlevel/2009/12/doe-v-netflix.pdf.

impact of this rule to industry is therefore not nearly as dire as some have painted it.¹¹ The rule would not ban any activity, instead it would require opt-in consent. Recent work suggests that companies have been very successful extracting consent even under similar opt-in rules.¹² If the Commission resists giving an ex ante blanket exception for nonsensitive information, ISPs will simply ask customers for permission to use their nonsensitive information in exchange for something that arguably benefits the customers. Indeed, if the proffered benefits are as good as ISPs have intimated, some consumers will probably consent to allowing access even to sensitive information.

Fourth, and finally, the industry trade association Future of Privacy Forum asks the Commission to create a multistakeholder process to define sensitivity.¹³ It cannot be overstated how awful this idea is. Multistakeholder processes for privacy have tended to fill gaps in the law, setting ground rules in areas where legislatures have not spoken with the same clarity as Congress has in Section 222. In addition, a multistakeholder process to define the sensitivity of data collected by ISPs would inevitably play out as a long, protracted deliberation in which privileged lobbyists debate the categories of information we ought to consider sensitive or not.¹⁴ Finally, this proposal suggests drawing the line between sensitive and nonsensitive information through a consensus-based process, raising the ugly specter of drawing these important lines by show of hands. This would base consumer privacy protection based on majoritarian concepts of sensitivity, leaving minority interests unprotected.

Sincerely,



Paul Ohm

¹¹ Reply Comments of Paul Ohm in the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (June 22, 2016), WC Docket No. 16-106, <https://www.fcc.gov/ecfs/filing/10622254783425>.

¹² Reply Comments of Professor Lauren E. Willis to Federal Communications Commission (June 27, 2016), WC Docket No. 16-106, <https://www.fcc.gov/ecfs/filing/1070776478772>.

¹³ Reply Comments of the Future of Privacy Forum to Federal Communications Commission (July 6, 2016), WC Docket No. 16-106, <https://www.fcc.gov/ecfs/filing/10706083993286>.

¹⁴ See David McCabe, *Facial Recognition Talks Break Down as Privacy Advocates Withdraw*, THE HILL (Jun. 16, 2015), <http://thehill.com/policy/technology/245098-privacy-advocates-walk-away-from-facial-recognition-talks> (“The advocates say that they found themselves at an impasse with industry representatives over whether companies should ever have to seek consent to use facial recognition on a user or person.”); Alvaro M. Bedoya, *Why I Walked Out of Facial Recognition Negotiations: Industry Lobbying Is Shutting Down Washington’s Ability to Protect Consumer Privacy*, SLATE (Jun. 30, 2015), http://www.slate.com/articles/technology/future_tense/2015/06/facial_recognition_privacy_talks_why_i_walked_out.html (“In Washington we have ‘no men’: industry lobbyists whose primary purpose is to stop attempts to regulate their members’ products and services, and who have no product or brand that could be hurt by their efforts. The tech industry can increasingly afford a lot of no men.”).